



IDENTIFICATION SYSTEMS FOR SOCIAL PROTECTION

 **ASSESSMENT MATRIX**



DELIVERY

The assessment criteria elaborated above should then be applied to the key areas. The assessment results should be captured in an overview table (assessment matrix) that captures key strengths and weaknesses in the performance of the identification system. The table below provides guidance on how to use the criteria and assess the performance from weaker to stronger.

Illustration of ID and CR System Assessment Results

	Latent	Emerging	Moderate	Advanced
<p>Accessibility</p> <ul style="list-style-type: none"> ● Coverage ● Inclusiveness ● Appropriateness <ul style="list-style-type: none"> – Cost of access and other barriers to access – Enrollment approach active or passive 	<p>Minority of the eligible population has an ID that can be used by the program</p> <p>Some vulnerable groups are de facto excluded from the ID system</p> <p>Acquiring the ID is costly in relative terms and administratively cumbersome (passive enrollment approach)</p>	<p>Most of the eligible population has an ID that can be used by the program</p> <p>Acquiring the ID is a burden for some groups of the population (e.g., the poor)</p> <p>Barriers to access are known (passive enrollment approach) and a strategy is defined</p>	<p>Almost all eligible people have the required ID</p> <p>Process of obtaining the ID involves low costs</p> <p>Concrete actions are taken to ensure access to the ID for vulnerable groups (active enrollment)</p>	<p>All eligible people have or can easily obtain the form of ID required for the program (including the poor, noncitizens, indigenous groups, etc.)</p> <p>A process is defined for the timely inclusion of newborns in the system</p> <p>The cost of obtaining the ID is low, and there are no other barriers to obtain the ID</p>
<p>Robustness</p> <ul style="list-style-type: none"> ● Uniqueness/accuracy ● Security ● Effective and reliable authentication procedures 	<p>Duplicates and other errors in the database are a major concern, as there is no process for deduplication and data cleaning</p> <p>Very low rates of birth and death registration/civil registry very unreliable</p> <p>IDs are easily falsified</p> <p>Very weak institutional capacity to ensure database security</p> <p>Authentication process very unreliable/dysfunctional</p>	<p>Some quality control and database maintenance but mostly paper-based recordkeeping</p> <p>Civil registry is functional, but low rates of birth and death registration and significant delays in registration</p> <p>Security measures are rather weak, and IDs can be falsified</p> <p>Authentication process unreliable</p>	<p>Data quality and deduplication protocols are in place and the database is reasonably accurate</p> <p>The majority of births and deaths is registered, and the civil registry works well with minimal delays</p> <p>Database security measures are in place, and IDs are rarely falsified</p> <p>Basic authentication processes</p>	<p>Electronic records facilitate quality control and deduplication; errors are minimal</p> <p>All births and deaths are registered in a fully functional civil registry that works with minimal delays</p> <p>Strong database security controls</p> <p>Very difficult to produce fraudulent IDs</p> <p>Good authentication standards applied</p>

	Latent	Emerging	Moderate	Advanced
<p>Costs of the ID system</p> <ul style="list-style-type: none"> ● Information technology ● Maintenance ● Ease of operation; administrator training <p>Interoperability and portability</p> <ul style="list-style-type: none"> ● Interoperability ● Portability 	<p>High cost</p> <p>Cost are disproportional compared to the benefits provided</p> <p>There is no standardized data format and little or no database linkages across programs; high dependence on local knowledge (e.g., community) and references for verifying identity</p> <p>The ID can be used only for one purpose and is tied to one locale</p>	<p>Some data are standardized, and a few major programs aim to make their databases compatible or use a common ID platform; difficult to track one individual across different programs</p> <p>There is a process to access benefits across the country, but it requires complicated administrative procedures and takes time</p>	<p>Most data are standardized, and some SP programs use a common ID</p> <p>Most program management information systems can be linked</p> <p>Accessing benefits at different points across the country requires paper work but is possible</p>	<p>Low cost</p> <p>ID costs are reasonable compared to the benefits provided</p> <p>To the extent that this is desired, interoperability across programs is fully functional, or SP programs use a common ID at the national level</p>



	Latent	Emerging	Moderate	Advanced
<p>Governance and Respect of Rights and Dignity.</p> <ul style="list-style-type: none"> ● Governance framework ● Institutional capacity ● Respect for rights and dignity <ul style="list-style-type: none"> – Data protection – Effective and accessible redress mechanisms in case of abuse, lack of due diligence, or wrongdoing 	<p>Roles and responsibilities for ID are not clearly assigned, and the ID process is not well implemented</p> <p>Infrastructure and the number and skills of staff are entirely insufficient</p> <p>Ad hoc or nonexistent mechanisms for privacy and data access</p> <p>No redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing</p>	<p>Roles and responsibilities are assigned to certain institutions, but they do not perform their functions as foreseen</p> <p>Infrastructure and the number and skills of staff allow ID processes to be carried out only partially</p> <p>Minimal protocols in place for personal data protection and privacy</p> <p>Redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing, but are not effective and accessible</p>	<p>The institutional and administrative framework clearly assigns roles and responsibilities, but there are complaints regarding delays and irregularities in implementation</p> <p>Infrastructure and the number and skills of staff are sufficient to carry out most of the ID process</p> <p>Most internationally accepted personal data protection standards and protocols are followed</p> <p>Mostly effective and accessible redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing</p>	<p>An effective institutional and administrative framework clearly assigns and enforces roles and responsibilities</p> <p>Infrastructure and number and skills of staff are sufficient to adequately carry out all ID processes</p> <p>Full compliance with internationally accepted personal data protection guidelines</p> <p>Fully effective and accessible redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing</p>

